PHRG
PEACE HUMAN
RIGHTS GOVERNANCE

Volume 5, Issue 1, March 2021

Digital Technology: Protection and/or Economic Value for Personal Data Knowledge and Management and Conformity to Soft Law Norms

Cristiana Carletti

Policy Papers

DOI:

10.14658/pupj-phrg-2021-1-5

How to cite:

Carletti, C. (2021) 'Digital Technology: Protection and/or Economic Value for Personal Data Knowledge and Management and Conformity to Soft Law Norms', *Peace Human Rights Governance*, 5(1), 125-150.

Article first published online

March 2021

PADOVA UP

PHRG 5(1), March 2021

Digital Technology: Protection and/or Economic Value for Personal Data Knowledge and Management and Conformity to Soft Law Norms

*Cristiana Carletti**

Abstract
Digital data flows have increased at a very fast pace: virtually they are more accessible but also more exposed to the risk of fragmentation, incorrect or incomplete acquisition and use for conflicting purposes by public and private actors. This has encouraged an interesting debate, fuelled by academic contributions and operational/models proposals from International Organizations and States: stimulating reflections have covered the relevance of soft law norms and their legal potentiality to create a proper and balanced systemic framework for the collection, storage and management of personal data by balancing the protection of human rights of data holders. The aim of the contribution is to preliminarily assess if soft law norms are really instrumental to protect the right of privacy and personal data as well as to reinforce their economic digital power.

Keywords: *human rights, right to privacy, personal data, digital technologies, digital space, economic value, soft law norms*

* *Associate Professor of International Law, Roma Tre University – Department of Political Science, cristiana.carletti@uniroma3.it*

Introduction

On a preliminary stage the collective and social dimension stays upon the recognition and substantive definition of individual rights in order define interpersonal relationship as well as the accomplishment of personal interests.

Indeed, traditional social relationships are based on the morality principle for codifying other values and interests and confirming individual freedoms as limited by collective ones. Morality is linked to the concept of respect, as a personal attitude which also implies self-respect so that the relationship can be socially appreciable. When respect is contextualised in a social order, traditional rules are legalized in such a way to introduce the right to control over individuals, in a physical and figurative sense. Meanwhile the social dimension critically impacts over the concept of confidentiality. If it is true that personal data sharing is agreeable, it yet requires the protection of human dignity and the intimate condition of the individual. At the same time, it is essential to formulate a specific legal status that allows to regulate interpersonal relationships in a social setting, defining in advance which behaviour to adopt and which actions to take.

The definition of confidentiality as a key-component of the legal formulation of the related right to privacy moves from the identification of the person concerned and involves its content and space-time parameters for proper implementation, including limited enjoyment of the right itself.

If confidentiality is clearly associated with personal data, particularly as per its individual dimension, on the other hand contemporary digital information and communication tools question its original definition and alter its effective protection. This further facilitates a broadening of legal contents to include the collection, management and protection of personal data as a whole; from this point of view, the protection of confidentiality undergoes a material expanding and necessary balance in respect of other rights and freedoms. So far the concept then be interpreted in its evolutionary significance in terms not only for an extension but also of personal autonomy and data ownership in respect of other individuals.

The nature of personal data, originally framed in limited circulation and management, today requires a wider investigation according to the potential and development of information and communication tools (ICTs) due to the amount of data flows outside traditional and physical boundaries. Reference should be made, in particular, to the so-called 'big data' and quantitative results as for data production and sharing (metadata).

In this view, even elementary mathematical syntax to build digital space and to progressively introduce data and information can be outlined in

relation to the impact of new technologies on moral values, confronting high criticalities as for the need to adapting information semantics to the Internet (Sullins 2021).

The reasoning proposed in this paper also moves from the tension between the need to regulate digital governance, whose rules - more soft than hard - require some form of compliance, and to introduce the concept of digital ethics. The latter, in fact, is not only the evaluation of the moral component related to information and digital communication, but also encompasses the chance to debate on legal, social and economic issues concerning values, rights, duties and responsibilities of actors on the Internet (soft ethics), and to encourage the process of formulation and adoption of both self-regulation (for private actors) or binding regulations (for public actors) for data flows, particularly personal data, on the Internet (hard ethics) (Floridi 2018).

Recent debate has focused on the analysis of the social and economic governance of Internet and regulation of web contents to ensure the full enjoyment of freedom of expression, information and communication within a democratic digital setting, but also the freedom to use Internet to provide and receive information without compressing the right to privacy and the protection of personal data (Brown 2010; Lucchi 2014; Oddenino 2008).

Starting from new challenges of digital technologies, the most appropriate compromise to request for mobilization of personal data should encompass the settlement of fundamental principles, rights and freedoms and their potential compression only where it is reasonable and justified on the Internet. This aspect will be explored in the first part of the paper.

Along these lines their economic relevance should be both preserved and enhanced, as requested by private actors working in the digital space scenario. Indeed, when these challenges have called for a comprehensive legal framework, an hard law reply has been provided by some Countries and, as it is the case, by the EU framework.

The adoption of Directive 95/46/EC placed the issue of sovereignty at the centre of the definition of European digital policy as a precondition for the regulation and control of digital technologies and the monitoring of societal effects, including a preliminary economic assessment. In this first stage, however, the static approach towards the protection of fundamental rights, and in particular of the right to privacy, stands out. Only by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), a comprehensive and complex legal framework has been provided at internal level and with regard to EU external relations, covering both personal data processing and data flows

from data holders and operators, whether public or private ones. It is precisely recital 7 of the Regulation that refers to the economic value of personal data processing: 'Those developments require a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market. Natural persons should have control of their own personal data. Legal and practical certainty for natural persons, economic private operators and public authorities should be enhanced'. Through the following step of the EU strategic priorities, e.g. the Digital Agenda for Europe (Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2010) 245 final/2, 26 August 2010), only in recent times the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Shaping Europe's digital future (COM(2020) 67 final, 19 February 2020) has defined a new framework, marked by a liberal impulse that takes due account of the dynamism of digital technologies and which is guided by regulatory requirements and the harmonisation of legal instruments by Member States and at European level. In this context the EU Strategies have come into being for data protection (A European strategy for data, COM(2020) 66 final, 19 February 2020) and cyber-security (The EU's Cybersecurity Strategy for the Digital Decade, 16 December 2020), and for an economic – also personal - data flows vision (Digital Service Act, COM(2020) 825 final, 15 December 2020; Digital Market Act, COM(2020) 842 final, 15 December 2020).

To date, in the drafting process of the Data Governance Act *(*Proposal for a Regulation of the European Parliament and of the Council on European data governance, COM(2020) 767 final, 25 November 2020*)*, the points raised in the Communication from the Commission to the European Parliament and the Council on 'Data protection as a pillar of citizen empowerment and the EU approach to digital transition: two years of application of the General Data Protection Regulation' (COM(2020)264 final, 24 June 2020) are significant. While appreciating the commitment of EU Member States to the functioning of the new cooperation and consistency mechanisms introduced by the Regulation, it is clear that 'the development of a truly common European data protection culture among DPAs is still an ongoing process', and a quite similar consideration over the opportunities for legislative harmonisation and inter-state cooperation is also made with reference to private actors as for the adoption of codes of conduct, certification mechanisms and standard contractual clauses in line with the Regulation.

Despite relevant legal results achieved within the EU, this framework won't be further explored in the contribution. Undoubtedly, the final consideration of the aforementioned Communication suggests a different analysis, proposed in the second part of this paper, driving the debate within international systems: the push to support the concept of 'Data Free Flow with Trust' in multilateral intergovernmental fora. The trust, as later explained with regard to OECD, moves from soft law norms as a preliminary step for an overall and noticeable attempt for a legal systematization of the matter by international players, i.e. International Organizations and States in their dialogue with ICTs private actors.

1. Dynamic Information and Communication and Data Digitalization Processes

The defence of confidentiality and personal data entails the reinforcement of the level of protection and is related to the wider range of services for this purpose. It is based on the awareness of how data are collected, entered and managed by the user following his/her consent (Siano Montuori 2016; Thobani 2018, 203-205).

However, the user does not always have the possibility to consent for data sharing in line with clear and transparent functioning of technological online and offline tools; nor does this condition imply full knowledge of improving changes adopted by digital managers over time, which affect negatively the protection of confidentiality and personal data.

Moreover, personal data sharing takes place by the (conscious) will of the manager and the user. The latter may sometimes be unaware of it: this occurs, for example, when a cookie is simply facilitated for better accessibility and functioning of the network, or when data are moved very easily and quickly to another digital platform (i.e. via the cloud), the data owner and user being not informed and consenting to this process (Kuan et al. 2011; Lanois 2011). Systems in place for receiving, storing and encrypting information or new tools and technological equipment purchased by the user will escape the principle of open data sharing in the future: it will be detrimental for the level of security, confidentiality and protection of personal data.

1.1. Basic Concept: Personal Data

With specific reference to personal data, the speed of information entered and shared on the Internet could not be directly related to traditional notions of data departure and arrival and monitoring mechanisms. In fact data mobilization is cross-border well beyond physical barriers or obstacles

(Aaronson 2018). Henceforth the development of national and international laws has focused over the correlation between the concepts of data transfer, sharing and limitations because personal data contents, their protection and respect for confidentiality could be compressed.

In this sense the Organisation for Economic Co-operation and Development (OECD) has reviewed in 2013 its Guidelines on privacy protection and cross-border flow of personal data, the latter concept defined as follows 'Transborder flows of personal data' means movements of personal data across national borders'. Furthermore, to ensure a proper and full personal data sharing: '17. A Member country should refrain from restricting transborder flows of personal data between itself and another country where (a) the other country substantially observes these Guidelines or (b) sufficient safeguards exist, including effective enforcement mechanisms and appropriate measures put in place by the data controller, to ensure a continuing level of protection consistent with these Guidelines'. Potential limitation of personal data flows are provided as: '18. Any restrictions to transborder flows of personal data should be proportionate to the risks presented, taking into account the sensitivity of the data, and the purpose and context of the processing'.

In the Council of Europe Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, Art. 12 is expressly dedicated to this aspect with reference to its implementation at the domestic level according to the principle of free movement of personal data with possible and admissible exceptions: '2. A Party shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorisation transborder flows of personal data going to the territory of another Party. 3. Nevertheless, each Party shall be entitled to derogate from the provisions of paragraph 2: a insofar as its legislation includes specific regulations for certain categories of personal data or of automated personal data files, because of the nature of those data or those files, except where the regulations of the other Party provide an equivalent protection; b when the transfer is made from its territory to the territory of a non-Contracting State through the intermediary of the territory of another Party, in order to avoid such transfers resulting in circumvention of the legislation of the Party referred to at the beginning of this paragraph'.

Massive access to a large number of data and information may not be impaired as a result of compression of digital security, affecting the authentication and integrity of data. This could also entail a possible limitation of confidentiality and personal data by the manager when, for example, the user does not employ an *ad hoc* network system such the Internet of Things or does not explicitly and appropriately express his/her consent for this purpose.

1.2. Confrontational Concepts: Data Authenticity and Integrity *vs.* Big Data

At present, special research is being carried out in the world of technology in order to create and implement new tools to improve the sphere of confidentiality and personal data by ensuring their authenticity and integrity. This is an essential precondition for dealing with the necessary and systematic regulation of the Internet of Things in a legal dimension, based on global system's functioning, multiple users and technologies being applied to confidentiality and protection of personal data (Atzori et al. 2010; Giusto et al. 2010). To this scope, moving from supranational and self-regulatory rules legal literature has proposed to work upon a legislation that guarantees the right of the user to know about: personal data collection and use; the legal prohibition of the Internet of Things in certain circumstances; a legislation that strengthens technological security and that supports and invests in technological research, also to pursue economic advantages (Weber 2010; Sicari et al. 2015).

In fact individual relevance on the Internet might assume an economic value in relation to personal data. This issue has already raised numerous debates, in view of the pre-eminent legal dimension of the right to privacy and protection of personal data in front of their misuse for the achievement of economic profits. Moreover the economic component is widely considered with reference to the virtual expansion of the Internet and digital platforms where the quantity of data strongly emerges if compared to the preservation of their quality.

In this sense personal data sharing both offline and online out of any space-time parameters is related to the so-called 'big data' in terms of size, production and use (van der Sloot et al. 2016; van der Sloot and Van Schender 2016).

Generally speaking, big data could be distinguished from small data by the direct reference to a vague number of people, whose data are aggregated and therefore connotated by anonymity, impersonality and non-sensitive relevance. This does not infer data material value: indeed, correct use of big data brings useful individual and collective/social benefits and prevents possible alterations to equality in the access and use of data and information. In this perspective, in public and private sectors positive effects could be achieved by the strengthening of principles of transparency, security and the provision of targeted and personalised services, moving from full knowledge of data concerning certain categories of users. This approach is valuable in the public administration, in the health sector, in basic services, in the field

of geo-localisation and the security and user-friendliness of transport nets, in advertising and online trade.

According to the technical definition of big data, which is based on volume, speed and variety (Laney 2001), the issue should be deeply explored.

The quantitative component reminds to the size and implies the creation and use of software for the insertion, compression and management of big data, with systemic updating and renewed potential due to rapid evolution of technological knowledge. This, however, does not exclude that technological products are partially operative, putting at risk data protection, information accuracy, the awareness of the users who have a more marginal role in the formulation of their consent over data use and processing in big platforms. Size also includes the number of sources producing and disseminating data: platforms for storing public and private shared data, social media, databases owned and managed by research centres, personal use of computers, tablets and smartphones. Data input and sharing is extremely quick and this determines the large volume of global exchange of information and communications. This must not take place by impairing awareness about a fair Internet use for data sharing, especially when they are personal and sensitive.

Therefore, to ensure that the right to privacy and protection of personal data are not undermined in the context of big data, it is crucial that regulatory measures are effectively applied (Kuner et al. 2012). To pursue this aim distinctions between small and big data do not imply a real anonymisation of data. Indeed, the insertion, processing and management of big data may take place preserving and appraising small data and personal profiles to facilitate their new personalisation in spite of full anonymity. Moreover, in the management of big data including qualitative evolution of new technologies, operational flexibility must not necessarily be considered prejudicial to the protection of confidentiality and personal data. In this perspective, aimed at improving platforms for storage and management of big data, it is also important to ensure the preservation of data integrity, so that both the manager and the user are satisfied with data completeness, updating and accuracy.

Along these considerations, an interesting debate has been promoted by both public and private actors on the need to outline a new legal framework for better regulation of activities related to big data, being wary of any possible adaptation of current regulatory measures for the protection of confidentiality and personal data. Some important aspects emerged in the discussion (Rubinstein 2013; Della Morte 2018).

In the context of big data, the traditional distinction between personal and non-personal data or data and metadata is inappropriate, as the useless

speculation on the need to ensure data which do not have a personal qualification and could be anonymous. So far, along the quantity of data collected and stored, the regulation of monitoring methods for data use, as well as the risks from inappropriate management to the detriment of data validity and integrity, managers' and/or users' accountability are key-actions (Carsten et al. 2018). Obviously, nothing can affect the negative potential of big data more than the global concern of the user for the compression of principles of transparency, control and accountability for data protection and management. This has so far slowed down the transformation of basic components of big data into specific legal instruments to regulate this sensitive issue, depersonalisation and anonymity procedural software tools, identification of both best ways - and also exceptions - of data sharing consistently with the primary sharing purposes and possible measures to reduce the risk of violation of the protection of confidentiality and personal data.

2. Digital Technology: Protection and/or Economic Value of Knowledge and Management of Personal Data

According to traditional communication tools all principles, rules and common guidelines have always been defined and implemented by public and private actors to determine the correctness of virtual dialogue from a legal point of view and a joint and mindful sharing of information facing collective and social needs.

Due to an increased data flow in the digital space, these actors had to correct and integrate the same principles and rules so that traditional communication could include new public and private players, without any territorial parameter. This has undoubtedly made data more accessible but also more exposed to risk of fragmentation, incorrect or incomplete formulation, acquisition and use for purposes other than those previously established.

Hence personal data have been evaluated not only as an information tool *tout court* but also as a cognitive tool assuming an economic and commercial value according to collective interests (Nissembaum 2009).

On a general note communication has a twofold advantage: for the benefit of the data holder, who collects, preserves and manages personal data in the digital space and must use the most suitable technology to protect them, even when he/she is committed to its development; for the benefit of each interested party, who is also a potential user and who acts for preserving his/

her digital identity and for choosing autonomously and voluntarily when the technology can and must anonymize data.

In this relationship, the data holder and the interested party interface according to mutual trust as an essential prerequisite of their dialogue. The trust relationship is based on the coexistence of primary requirements such as: ease of access to digital space and control of personal data for the interested party; ordinary and permanent relationship between actors to increase trust; investment in structural and operational technological tools by the data holder; adherence to a set of principles and rules to inform correct collection, storage and management of personal data (Etzioni 2019).

If the interested party builds a real relationship of trust and places a strong expectation on the data holder, the latter is able to work constructively, developing the digital space and technological tools at his/her disposal so that data sharing risks are minimized. This process includes actions aimed at expanding the digital space that require little anonymisation, careful multi-level - direct and mediated - data collection, storage and management, control over personal data online and offline, transparent access to data for the interested party if the holder proceeds to create new digital platforms for commercial purposes or technological tools aimed at certifying activities encouraged and carried out on these platforms.

2.1. From Digital Communication towards the 'Economy of Privacy'

Along these considerations, it is clear that opportunities offered by the development of the digital space and the relationship of trust between data holders and interested parties have facilitated an economic point of view about knowledge and management of personal data.

The so-called 'economy of privacy' is based on the awareness of the economic value of data in a way that is very far from theoretical speculation over the prevalent legal scope of the right to privacy, involving the determination of limits between data sharing and their concrete and effective protection (Cecere et al.2017).

Generally speaking, the 'economy of privacy' produces positive effects in relation to the expansion of opportunities for the creation, transmission and open sharing of personal data and has a security significance if both parties involved in the trust relationship are aware of the need to deal appropriately with asymmetric alterations. In this context they are called to contextualise data knowledge from an inter-temporal point of view, in the expectation that its economic value is dynamic and that economic estimate of sharing and

protection is directly remitted to the market (for an in-depth recent analysis on this matter Nakamura et al. 2018).

However, the 'economy of privacy' also implies a distinction of perspective between the two actors, also in order to prevent the above-mentioned relational asymmetry: this often depends on how data are used, often not transparently enough to allow the interested party to be aware of the sharing process (Acquisti 2014).

Indeed, the economics of personal data firstly presupposes such awareness on behalf of the interested party: he/she, in fact, may not agree with cost-benefit evaluation of data sharing, possible decrease of costs to access to market services, trade operations and data sharing evolution, expected and achieved results in the trade market (Murphy 1996; Li et al. 2019; Nguyen and Paczos 2020).

Awareness of the data holder, on the other side, might consist of better knowledge about consumer's attitudes to direct the flow of trade goods to the benefit of the potential or real individual and collective buyer, or about personal data sharing often unknown to the interested party. Likewise, the data holder must always and in any case observe the evolution of data flow volume, which has a specific impact on direct and indirect/anonymised data sharing in economic terms. It is also important to assess the cost on behalf of the holder for data collection, management and sharing against occasional losses due to the violation of confidentiality and additional legal and compensation expenses in favour of the interested party as well as reputational losses that can be assessed in quantitative terms.

This conceptualisation of the 'economy of privacy' has assumed a different relevance over time, especially from a digital space perspective.

In a first phase personal data have been attributed a specific commercial value, according to the level of protection guaranteed by the data holder. In a second phase, the economic component prevailed over the need for protection: in this sense, the data holder opted for a noticeable development of digital technologies, entailing a significant economic bulk on the market; so far there was an easier data entry into the market as well as the attribution of a commercial value, both when data are shared directly and through indirect holders - as occurs for the namely private actors on digital trade platforms. On a final stage, today digital technology has evident economic bulk. In this context, the market has adapted to the good, i.e. digital data. Digital data do not meet the criteria of uniqueness in terms of location: personal data market is complex and decentralized. Moreover data are marketed and made accessible to interested parties in different trade sectors; data can become an information tool among owners as users for access to free goods and services; data are employed by users as consumers to purchase technologies

aimed at guaranteeing a strengthened data protection; data can be shared in the market by users as consumers to incentive purchase and sale circuits.

Therefore, in current times the 'economy of privacy' involves, beyond the data holder, the producer as actor that collects, preserves, manages and shares personal data influencing market trends in a profitable way both for the development of technologies and for data protection; while the interested party, acting as a consumer, has a similar function by giving more incentives to the market to safeguard data.

2.2. 'Economy of Privacy' (Self)rules for Security Purposes

In order for the 'economy of privacy' to regulate the market in a correct and effective way, it is important that the economic model can adapt to trade trends on the basis of suitable self-rules to monitoring costs and goods mobilization (Bauer et al. 2016; Martin and Murphy 2017).

A self-regulation regime presents undoubted advantages when it makes trade players preventively accountable, urging them to pay attention to possible risks for personal data on the market, significantly differentiating the purchasing power and the volume of transactions of small and large public and private actors. But this could easily result in an increase in the costs of data collection, storage, management and sharing and, consequently, of services of access and protection of personal data - today often free of charge.

There is no doubt that massive flow of data and new opportunities offered by the expansion of access to databases managed by both public and private actors can alter the trust relationship among data holders, interested parties, data producers and consumers, benefiting alternatively the economic growth of the market or the level of protection of personal data. This option has pushed for the transition from an 'economy of privacy' to an 'economy of security' (Tao et al. 2019). If the data holder is required to make substantial investments to strengthen the level of protection of personal data, to combat all forms of illegal activities to the detriment of personal data and to prevent possible costs arising from inadequate data protection management, it follows that analysis and business planning must include the beneficial parameter by providing for greater use of financial resources and reputational instruments, supplemented by a review of principles and self-regulation in favour of business ethics.

If the 'economy of privacy' is combined with the 'economy of security', the balanced result that takes into account both economic development and personal data protection can be translated into the so-called 'business of privacy' (Mantelero 2007). In this sense, the right to privacy is no longer

perceived as an obstacle to business development, but rather as a possible source of income. In this way, the economic value of personal data, pursued by the data holder and endorsed by the interested party, is the basis of a process aimed at attributing a proper value to personal data.

2.3. The good compromise: 'business of privacy'

First of all, the economic component emerges in relation to potential investment of the data holder in order to ensure a higher level of protection of personal data, by activating security measures and assuming specific management figures: in this approach it is entirely convenient and in line with individual and collective interest.

Moreover data sharing must take place in accordance with the above mentioned trust relationship. In these circumstances the economic value of sharing resides properly in the level of protection: personal data, as a product, are guaranteed and have an economic relevance. When choices are made immediately or when Internet access is facilitated, without considering negative effects in the medium and long term, trade activities are encouraged. On the contrary, marketing of digital services is depreciated when the protection is not guaranteed in an all-inclusive manner or when data are shared because, for example, their use is aimed at achieving purposes other than the original ones.

To avoid similar situations, the 'business of privacy' requires a specific regulation involving the data holder and the interested party as a potential user of the service.

In this context, the latter may express his/her consent both explicitly and implicitly. In the first case, he/she is often not fully aware about the formulation of his/her will: the consent is formulated in both direct and indirect form or may undergone into a specific dialogue with the data holder for the purpose of its best formulation. In the second case, new implicit formulas have been introduced by the data holder in such a way to overcome this step, however without excluding procedural amendments. In a completely paradoxical way, in the face of explicit consent, the interested party is aware of the procedure but does not have transparent access to information on data sharing quantitative and qualitative methodologies; on the other hand, when the interested party gives his/her implicit consent, he/she is not at all aware of critical issues in terms of potential violations of his/her right to confidentiality.

In order for the 'business of privacy' to be concretely beneficial for data holders, interested parties, data producers and consumers, the most appropriate legal solution is the negotiation and adoption of an *ad hoc*

contract model in compliance with national legislation and international standards in force for the right to confidentiality and protection of personal data; the sharing of personal data is carried out on the basis of the potential recipient and consumer and the informative nature - generic or sensitive - of personal data (Wright 2019). In an even more detailed formulation of the contract model, the relationship between the data producer controller, the data holder and the interested party is declined by introducing an obligation to safeguard data by the producer and controller, beyond any trade data sharing profit.

However, the model may face numerous problems - and this is an important element that entails an in-depth analysis on the 'business of privacy' in general - in the process of collecting, storing, managing and sharing a large amount of personal data (Zeno-Zencovich and Giannone Codiglione 2016).

Indeed, prior or contextual intentional personal data sharing and related concrete awareness of the risk of sharing is lacking. So far, a proper functioning of the 'business of privacy' should guarantee enhanced monitoring and ongoing adaptation to new digital technologies. The data producer and controller is recommended to advance in this area: any form of investment is generally made easier by a complex and capital-intensive system that strikes a fair balance between the collection and management of personal data, security and protection of the privacy of the data holder, interested party and user. But this scenario might facilitate large companies which, especially in the field of new digital technologies, could take dominant positions by altering principles and basic rules of the competition system to the detriment of small businesses. Digital technologies, as a trade sector, are not free from such practices: private digital managers purchase an extensive information patrimony to influence market trends. If originally digital neutrality, free from constraints and limits, was real today, on the contrary, the economic interest clashes with the need to protect privacy and personal data. Therefore, all public and private actors must act in such a way as not to negatively affect the economic value of the good - personal data - ensuring its accessibility and quality in a truly competitive and self-regulated system.

3. Soft Law Norms: Some Preliminary Remarks

The evident quantitative and qualitative dimension of collection, storage and management of personal data entails some critical issues involving international hard and soft norms within the main intergovernmental systems for an effective protection of confidentiality and personal data.

In comparison with traditional legal standards about digital challenges and human rights protection, a different analysis could be proposed about the relationship among principles, rights and technologies for a proper regulation of data sharing.

The moral and ethical component is significant to this purpose: digital technologies work out of any legal/hard reference (i.e. for sharing and open access to information) to get economic profits in spite of the protection of data holders users, leading to an individual profiling that is even more damaging to their confidentiality.

Therefore, due to lack of hard laws governing the role and actions carried out by public and private players, personal data collection, storage and management give rise to a voluntary processing. In such circumstances operational ethics implies that directly concerned persons (and indirectly concerned individuals within a community) is in any case informed about processing methods and results produced by technological anonymised tools, such as artificial intelligence (among others: Gurkaynak et al. 2016; Fasan 2019; Finocchiaro 2019) and algorithms (Kroll et al. 2016).

To avoid arbitrary conducts by data holders and producers, advancement of new digital technologies must include preliminary, contextual and subsequent operational measures, ensuring full compliance with the principle of transparency to justify the choice and adoption of algorithmic methodologies. This changeover let also to reflect upon the development of appropriate legislative and policy instruments with the participation of both the data holder and the interested party. Indeed the latters can provide for insightful comments to ensure the moral and ethical relevance of the topic also by a legal standpoint.

All possible solutions are not free from any risks. In fact, new digital technologies are rather complex, are featured by strong procedural automatisms and are mainly managed by private actors. Even if technological innovations are always configured and made feasible by a human factor, this has a decisive influence on the functioning - albeit discriminatory - of personal data collection, storage and management. To overcoming these risks a real objectification of the process and a pre-evaluation of factors affecting its malfunctioning in a moral and ethical perspective are necessary. It should be completed by introducing risk assessment models (or 'ethics in design') to impact on the re-formulation of traditional rules and legislative measures (Wight and Mordini 2012; Mantelero 2018; Tamò-Larrieux 2018).

Henceforth, combining the dynamism of technological development and the need to protect human rights - including the right to privacy and personal data - some soft regulation models with a moral and ethical vocation are a valid alternative aimed at filling the regulatory gap to govern the conflictual

relationship between technology, principles and rights. In this sense soft law norms could be instrumental in order to: prevent risks for a potential use of personal data for purely economic purposes; predict malfunctioning of decision-making mechanisms; promote development of procedural models based on the quality and security of personal data; relaunch the drafting and adoption of legal measures to better regulate the right to privacy and data protection while advancing for profitable economic benefits (DeCew 1997).

4. The Elaboration of Soft Law Norms for an Appropriate Regulation of the Matter in an Economic Perspective

A targeted process aimed at drafting soft law norms including principles and rules for the confidentiality and protection of personal data and governing transboundary data management in an economic perspective has been carried out within the framework of the Organization for the Economic Cooperation and Development (OECD).

A specific Group of Experts (the so-called 'Data Bank Panel') was set up in 1969 to this end, with the task of examining the confidentiality component of the Programme on cross-border data flows through the use of ITCs support. The Group compiled and published a series of *ad hoc* studies dedicated to topics such as 'Computerised Data Banks in Public Administration', 'Digital Information and the Privacy Problem' and 'Policy Issues in Data Protection and Privacy'. A workshop was held in 1974 to discuss these topics in order to find suitable soft regulations, leading to a special focus on the economic dimension of data sharing debated during an additional Workshop organized in 1977. In this occasion a number of principles emerged such as: free circulation of information, possible exceptions to data flows due to security reasons or their non-compliance with national legislation and citizens' rights, recognition of an intrinsic economic value of personal data and therefore the need for 'marketing in compliance with the rules of trade competitiveness, personal data protection in case of unfair use or sharing'.

The recognition of these principles by a new Group of Experts, established in 1978 (the so-called 'Group of Experts on Transborder Data Barriers and Privacy Protection'), launched the drafting process for a non-binding legal instrument, the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, in collaboration with the EEC and the Council of Europe. The Guidelines were adopted on 23 September 1980 to govern the protection of privacy and personal freedoms and the, transboundary data flow and related economic and social benefits.

4.1. The Guidelines on the Protection of Privacy and Transborder Flows of Personal Data: a Preliminary Step

In compiling the Guidelines, the Group of Experts has defined some key aspects: a general approach for multiple data collection, storage and management activities; the nature of the interested natural and legal party; the creation of judicial and quasi-judicial control systems and mechanisms; lack of international standards and the implementation of national legislation in force persecuting breach of confidentiality where it takes place; identification and determination of possible general or special exceptions for the right to confidentiality; challenges for the domestic implementation of the Guidelines.

In general terms, the Guidelines proved to be instrumental for the achievement of core-targets, particularly that one to assume the aforementioned principles and values as the lowest common denominator for the harmonisation of domestic legislations and for the regulation of the cross-border data flow in a cooperative, reinforced and expansive manner.

Moving from a comprehensive conceptualization of the issue (i.e. automatic/non automatic data controller, natural and legal interested party, transboundary personal data flow), even according to a soft legal approach, the Guidelines provide some insights to limit their discretionary implementation by national authorities - such as 'national sovereignty, national security and public policy ('ordre public')' - to inform the adoption of domestic legal measures for the protection of privacy. In Part Two of the Guidelines, personal data collection, storage and management should are required to be carried out legitimately and correctly, ensuring the knowledge and consent of the interested party. In this process the quality of personal data, their targeted and transparent use and related limits, accuracy, completeness and updating must be guaranteed, making the data holder and producer accountable for all these actions. The domestic location of the data holder entails the relevant role of national authorities for an harmonization of legislations on personal data collection, storage and management in the event of cross-border transfer to another State, as Country of transit or destination: this approach include open access and dynamic use of data but also possible limitations when legislative measures are not equivalent in providing a proper data protection. So far, due to the fast evolution of new technologies, sharing of information as well as the adoption of clear and simplified procedures for mutual assistance in the event of non-compliance with the Guidelines are crucial.

The response from OECD Member States in implementing the Guidelines has been composite: general or specific legislative measures, self-regulation

rules, the establishment of national bodies in charge for implement and monitor compliance with the Guidelines are just some of the examples of their reception and impact. Indeed, national authorities have faced a huge technological development process as well as an impressive extent of ICTs devices, an increase of data flow lines and networks, lower costs of data storage and management equipment - partly due to a strong delocalisation of services, most sophisticated and automatised mechanisms for the collection and storage of personal information up to a potentially unlimited data volume. Hence States have been bound also to pay attention on economic and social effects of technological development and have faced new business management models facilitated by the completeness and speed of data flows, making the demand & supply chain out of traditional space-time parameters.

This has led to review soft law norms yet in place to search for a good balance among personal data protection, digital development and economic opportunities.

4.2. The Revised Guidelines for the Security of Information Systems and Networks

Again, within the OECD the Guidelines for the Security of Information Systems and Networks have been adopted in 1992: this is the first proposal for a 'privacy management framework' addressed to public and private actors for the definition of policies, procedures and systems for the protection of personal data, under periodical monitoring and evaluation. On a later stage, the high level of protection of privacy and personal data has been at the core of the Recommendation on Cross-border Cooperation of 12 June 2007 on the implementation of legislative measures for the protection of privacy. The monitoring cycle for the implementation of the Recommendation has provided for the creation on 10 March 2010 of the so-called Global Privacy Enforcement Network (GPEN), equipped with a special digital platform for the exchange of knowledge, experiences and best practices, training activities. Furthermore, the adoption of the Seoul Declaration for the Future of the Internet Economy of 18 June 2008 represents another relevant step: this document highlights the close relationship among economic, social and cultural factors supported by ICTs and has encouraged the update of the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data by an *ad hoc* Working Party on Information, Security and Privacy.

The new edition of the Guidelins, adopted on 11 July 2013, marks firstly the definition of personal data and related effective protection through the use of anonymisation and de-identification techniques and pays special attention to the multi-actor nature of the data producer, controller and manager for

the compliance with possible but flexible limitations in the collection, storage and management of personal data in view of the extreme ICTs evolution and the extensive volume of data flows.

In general terms, the updated Guidelines made evident how the pre-eminent sectoral approach has affected the economic relevance of soft law norms, facilitating a stronger multi-actor cooperation for common economic purposes. However, many evolving technical factors, especially in the context of new digital technologies, have been and should increasingly be taken into account for the protection of privacy and personal data such as: the volume of transboundary data flows, traditional and innovative data analysis, major difficulties for data processing and preservation, a large number of public and private actors institutional in the digital space and their different data processing models according to economic parameters.

Notwithstanding these criticalities, through the adoption of soft law norms the OECD has carried out a significant systematization for the harmonization of principles and methodologies to be transposed by its membership for the purpose of guaranteeing the right to privacy and personal data uniformly.

4.3. Recent Soft Law Trends on the Matter within the OECD System

The constant search for a balance between the protection of privacy and personal data and storage, management and sharing of information through digital technologies and the Internet - as complex processes based on the recognition of data economic value - has led the membership of the Organisation to reflect again on this issue in recent times, albeit always through soft law norms.

By way of example, two documents can be mentioned. The first is the Ministerial Declaration on the Digital Economy: Innovation, Growth and Social Prosperity (Cancún Declaration). In this Declaration, the commitment of the membership is aimed firstly at encouraging free data flow in order to achieve various goals, which can be associated with human rights' protection while preserving Internet openness but also with the fulfilment of privacy and data protection operational frameworks. In this perspective soft regulation (or business ethics) based upon public-private partnership is captured. Public actors are called upon to preserve the open nature of the Internet through the implementation of policies impacting on privacy, security, intellectual property, so far corroborating users' trust; private actors are asked to act responsibly and transparently for digital security and privacy risk management practices. But there is also room for joint action beyond national borders according to the space-time dimension of the Internet: it

is aimed at 'develop privacy and data protection strategies at the highest level of government that incorporate a whole-of-society perspective while providing the flexibility needed to take advantage of digital technologies for the benefit of all; and support the development of international arrangements that promote effective privacy and data protection across jurisdictions, including through interoperability among frameworks'. The second relevant document is the Recommendation on Digital Security of Critical Activities, adopted by the OECD Council on 11 December 2019 on proposal of the Committee on Digital Economy Policy (CDEP). This Recommendation also reinforces the idea that the balance between the protection of privacy and personal data flows is left to the close cooperation between public and private actors: strengthening digital security is even more important in critical circumstances, where risk assessment and timely data management are crucial co-factors to protect the individual as Internet user. If public-private partnerships will provide for a high level of security in many sectors closely related to the use of ICTs, with 'clear aims, values and rules, mutual benefits over time, respect for privacy and personal data protection regulation as well as other regulation protecting the confidentiality of information such as trade secrets', then the individual trust towards the overall Internet governance can be strengthened.

Some Final Considerations

At present a wide academic multi-disciplinary discussion is on-going to prove that a future hard codification to regulate the process of collection, management and sharing of personal data, whether sensitive or not, could be based on self-regulatory provisions to guarantee the highest level of protection of individual rights and freedoms and to support a constant process of economic development along the technological dimension.

In particular the debate on the scope of international regulatory/hard norms started from a deep criticism: it is essentially based on legal fragmentation in the face of an increasingly wide and articulated use of new technologies overcoming boundaries, obstacles and physical limitations for open, transparent and dynamic sharing of data and information (Goldsmith 1998; Trachtman 1998). Henceforth all sort of alternative regulations have been featured with technical and soft commitments, sometimes envisaging the establishment of monitoring and control bodies without the power to investigate and sanction violations of confidentiality and standards for data sharing (Mody 2001; Odennino 2008). Also negative considerations from the academia concern the extreme evolution of new technologies and the

practical difficulty of freezing principles and rules granting confidentiality and personal data protection. On this point, nothing could prevent these principles and rules from being preliminarily defined for possible amendments for their concrete and effective adaptation to changing technologies and for feasible limitations and exceptions that are proportional, justified and limited in time.

The conduct of States on this matter, in terms of national sovereignty and with regard to the debate and the progressive development of international - soft or hard - norms within the main international intergovernmental systems, has been diversified.

On a general note they have contributed for the drafting and adoption of international hard and soft norms, in line with their legal principles and basic rules in force at the domestic level.

For example, they have adopted some negotiating flexibility for legal measures in compliance with international human rights law which have been translated into domestic principles and standards for confidentiality and protection of personal data. This behaviour was endorsed by many States Parties to the European Convention for the Protection of Human Rights and Fundamental Freedoms, letting the European Court of Human Rights to take action in front of the violation of the right to privacy and personal life - private and family life - to be protected in an appropriate and balanced manner with respect to other rights, in particular freedom of expression and information as per the digital space. In contrast, States have shown less flexibility in negotiating binding legal instruments ruling highly technical disciplines or involving preliminary assessments of the impact of rules to the detriment of technological development and economic interests of national public and private actors involved.

For all these considerations, digital space, principles and rules of virtual social coexistence (the so-called 'Internet governance') and related individual and collective rights have created new expectations: until now we have only experienced an extensive interpretation of key provisions contained in international human rights law to be revised in the light of the new individual and collective virtual rights and freedoms.

As demonstrated, OECD has approached this issue by giving it a global, technical and economic dimension. The result achieved has been translated into interesting soft law norms in order to identify correct balance between protection of the right to privacy and personal data, development of digital technologies and economic growth. This effort has partially overcome divergences from the view of States legislations and private actors self-rules. The specific relevance of soft law norms has not yet facilitated a valid affirmation of common principles and values for the protection of the right

to privacy and personal data: rules in force govern mainly the purposes and methods of data collection, the awareness of the data holder and the interested party regarding the storage and use of his/her personal data, the right to access and correct its content, the determination of the data holder to assess the conformity of his/her activity with legal standards and related accountability in the event of violation of the legislation in force.

To sum up, on the one hand the process for binding instruments has produced divergent results with regard to the right to privacy and the protection of personal data, in the attempt to contextualise them in the digital space. So far international human rights law has been implemented and monitored in a careful manner, investigating about the level of protection of rights and freedoms with respect to new technologies and the digital environment in limited case-law. On the other hand, sectoral and technical soft codification solutions have proved to be an interesting perspective in relation to the digital space: but they are limited as per their regulatory approach, which is cooperative in its nature and alternatively takes into account security or economic challenges. This limited relevance is also linked to the role of private actors in the digital space and their reluctance to adapt their conduct within a rigid and binding legal regime.

In any case the drafting and adoption of soft law norms should not be underestimated: indeed, they have contributed and are contributing for further interpretative solutions, trying to update their scope for an appropriate correlation with new need to guarantee the right to privacy and the protection of personal data in the digital perspective, as provided by international hard law standards in force.

Maybe it is precisely the multi-actors factor that can influence the start of a process of international hard codification of the matter which, as pointed out in the OECD system, may prove instrumental in the process of data governance for trust, e.g. ensuring data opening to be properly balanced against issues of privacy, security and economic benefits. The requirements concerning the obligations to protect the right to privacy and personal data on behalf of States and private actors imply a broader reflection for the elaboration at first of targeted self-regulatory rules and, in the future, hard legal measures in order to balance individual (privacy and personal data) and collective (economic) interests also in the digital space.

References

Acquisti, A. (2014) 'The Economics and Behavioral Economics of Privacy', in Lane, J., Stodden, V., Bender, S., Nissembaum, H. (eds.), *Privacy, Big*

Data, and the Public Good: frameworks for engagement, Cambridge, 2014, 76-95.

Aaronson, S.A. (2018) 'Data is different: Why the world needs a new approach to governing cross-border data flows', CIGI papers no. 197. Centre for International Governance Innovation, Waterloo, ON.

Atzori, L., et al. (2010) 'The Internet of Things: A Survey', *Computer Networks*, 54(15), 2787-2805.

Bauer, M., Ferracane, M.F., van der Marel, E. (2016), 'Tracing the Economic Impact of Regulations on the Free Flow of Data and Data Localization', Global Commission on Internet Governance (GCIP) Series paper No. 30, May 2016.

Brown, I. (ed.) (2013) *Research Handbook on Governance of the Internet*, Cheltenham: Edward Elgar Pub.

Carsten Stahl, B., Wright, D. (2018) 'Proactive Engagement with Ethics and Privacy in AI and Big Data - Implementing responsible research and innovation in AI-related projects', *IEEE Security and Privacy,* 16(3), 1-14.

Cecere, G., et al. (2017) 'The Economics of Privacy', *The New Palgrave Dictionary of Economics*, 1-11.

Council of Europe, 'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28.I.1981, European Treaty Series - No. 108', retrieved from https://www.coe.int/it/web/conventions/full-list/-/conventions/treaty/108 (accessed: 01/12/2020).

DeCew, J.W. (1997) *In Pursuit of Privacy: Law, Ethics and the Rise of Technology,* New York: Cornell University Press.

Della Morte, G. (2018) *Big data e protezione internazionale dei diritti umani. Regole e conflitti*, Napoli: Editoriale Scientifica.

Etzioni, A. (2019) 'Cyber Trust', *J Bus Ethics*, 156, 1–13.

Fasan, M. (2019) 'Intelligenza artificiale e pluralismo: uso delle tecniche di profilazione nello spazio pubblico democratico', *BioLaw J.*, n. 1, 101-113.

Finocchiaro, G. (2019) 'Intelligenza Artificiale e protezione dei dati personali', *Giurisprudenza Italiana*, 1670-1677.

Floridi, L. (2016) 'On Human Dignity as a Foundation for the Right to Privacy', *Philosophy & Technology*, 29 (4), 307-312.

Floridi, L., Taddeo, M. (2016) 'What is Data Ethics?', *Phil. Trans. R. Soc. A.*, 374: 20160360.

Floridi, L. (2018) 'Soft Ethics and the Governance of the Digital', *Philos. Technol.*, 31, 1–8.

Floridi, L. (2018) 'Soft Ethics: Its Application to the General Data Protection Regulation and Its Dual Advantage', *Philos. Technol.*, 31, 163–167.

Giusto, D., et al. (eds.) (2010) *The Internet of Things*, Amsterdam: Springer.

Goldsmith, J. (1998) 'Against Cyberanarchy', *University of Chicago Law Review*, n. 4, 1199-1250.

Gurkaynak, G., Yilmaz, I., Haksever, G. (2016) 'Stifling artificial intelligence: Human perils', *Computer L. & Sec. Rev.*, 32(5), 749-758.

Kroll, J.A., Barocas, S., Felten, E.W., Reidenberg, J.R., Robinson, D.G., Yu, H. (2016) 'Accountable algorithms', *University of Pennsylvania Review*, 165, 633–705.

Kuan Hon, W., Millard, C., Walden, I. (2011) *The problem of 'personal data' in cloud computing: what information is regulated?—the cloud of unknowing*, Oxford: OUP.

Kuner. C. et al. (2012) *'The Challenge of 'Big Data" for Data Protection', International Data Privacy Law*, n. 2, 47-49.

Laney, D. (2001) '3D Data Management: Controlling Data Volume, Velocity, and Variety', Gartner, file No. 949. 6 February 2001, http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf.

Lanois, P. (2011), 'Privacy in the age of the cloud', *Journal of Internet Law*, n. 6, 3-17.

Li, W.C.Y., Nirei, M., Yamana, K. (2019) 'Value of Data: There's No Such Thing As A Free Lunch in the Digital Economy', U.S. Bureau of Economic Analysis Working Paper, Washington, DC.

Lucchi, N. (2014) 'Internet Content Governance and Human Rights', *Vanderbilt Journal of Entertainment &* Technology *Law*, 16(4), 809-856.

Mantelero, A. (2007) *Il costo della privacy tra valore della persona e ragione d'impresa*, Milano: Giuffrè.

Mantelero, A. (2018) 'AI and Big Data: A blueprint for a human rights, social and ethical impact assessment', *Computer L. & Sec. Rev.*, n. 34, 754–772.

Martin, K.D., Murphy, P.E. (2017) 'The role of data privacy in marketing', *J. of the Acad. Mark. Sci.*, 45, 135–155.

Mazzucato, M. (2018) 'Let's make private data into a public good', in *MIT Technology Review*, 121 (4), 74-75.

Mody, S.S. (2001) 'National Cyberspace Regulation: Unbounding the Concept of Jurisdiction', *Stanford Journal of International Law*, n. 37, 365-390.

Murphy, R.S. (1996) 'Property Rights in Personal Information: An Economic Defense of Privacy', *Georgetown Law Journal*, 84, 2381-2417.

Nakamura, L., Samuels, J., Soloveichik, R. (2018) 'Free' Internet Content: Web 1.0, Web 2.0 and the Sources of Economic Growth', Paper prepared for the 35th IARIW General Conference, Copenhagen, Denmark, August 20-25, 2018.

Nguyen, D., Paczos. M. (2020), 'Measuring the Economic Value of Data and Data Flows', OECD Digital Economy Papers No. 297, OECD Publishing, Paris.

Nissembaum, H. (2009) *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford: Stanford Law and Politics.

Oddenino, A. (2008) *La governance di internet fra autoregolazione, sovranità statale e diritto internazionale*, Torino: Giappichelli.

OECD, 'Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data', 1980-2013, retrieved from https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (accessed: 01/12/2020).

OECD, 'Guidelines for the Security of Information Systems, 1992, retrieved from http://www.oecd.org/sti/ieconomy/oecdguidelinesforthesecurityofinformationsystemsandnetworkstowardsaculturesecurity.htm (accessed: 01/12/2020).

OECD, 'Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy', 2007, retrieved from https://www.oecd.org/sti/ieconomy/oecdrecommendationoncross-borderco-operationintheenforcementoflawsagainstspam.htm (accessed: 01/12/2020).

OECD, 'Seoul Declaration for the Future of the Internet Economy', 2008, retrieved from https://www.oecd.org/futureinternet/ (accessed: 01/12/2020).

OECD, 'Ministerial Declaration on the digital economy: innovation, growth and social prosperity ('Cancún Declaration'), 2016, retrieved from http://www.oecd.org/digital/Digital-Economy-Ministerial-Declaration-2016.pdf (accessed: 20/03/2021).

OECD, 'Recommendation of the Council on Digital Security of Critical Activities', 2019, retrieved from https://legalinstruments.oecd.org/api/print?ids=659&Lang=en (accessed: 20/03/2021).

Rubinstein, I.S. (2013) 'Big Data: The End of Privacy or a New Beginning?', *International Data Privacy Law*, n. 2, 74-87.

Siano M., Montuori L. (2016) 'Evoluzione del concetto di consenso informato nel mondo digitale e transizione del marketing tradizionale alle attuali sfide della profilazione', in Busia, G., Liguori, L., Pollicino, O. (a cura di), *Le nuove frontiere della privacy nelle tecnologie digitali*, Roma: Aracne Editore, 101 ss.

Sicari et al. (2015) 'Security, privacy and trust in Internet of Things: The road ahead', *Computer Networks*, 76, 146–164.

Sullins, J. (2021) 'Information Technology and Moral Values', *The Stanford Encyclopedia of Philosophy* (Spring 2021 Edition), Edward N. Zalta (ed.), https://plato.stanford.edu/archives/spr2021/entries/it-moral-values/ (accessed: 20/03/2021).

Taddeo, M., Floridi, L. (2016) 'The Debate on the Moral Responsibilities of Online Service Providers', *Sci. Eng. Ethics.*, 22 (6), 1575-1603.

Tamò-Larrieux, A. (2018) *Designing for Privacy and its Legal Framework. Data Protection by Design and Default for the Internet of Things*, Berlin: Springer International Publishing.

Tao, H. et al. (2019) 'Economic perspective analysis of protecting big data security and privacy', *Future Generation Computer Systems*, 98, 660–671.

Thobani, S. (2018) *Diritti della Personalità e Contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, Torino: Giappichelli.

Trachtman, J. (1998) 'Cyberspace, Sovereignty, Jurisdiction and Modernism', *Indiana Journal of Global Legal Studies*, n. 2, 561-581.

Van der Sloot, B., Broeders, D., Schrijvers, E. (eds.) (2016) *Exploring the Boundaries of Big Data*, Amsterdam: Amsterdam University Press.

Van der Sloot, B., van Schendel, S. (2016), *International and comparative legal study on Big Data*, WRR Working Paper number 20, The Hague.

Wight, D., Mordini, E. (2012) 'Privacy and Ethical Impact Assessment', in Wright, D., De Hert, P. (eds.), *Privacy Impact Assessment*, Amsterdam: Springer, 397–418.

Zeno-Zencovich, V., Giannone Codiglione, G. (2016) 'Ten Legal Perspectives on the "Big Data Revolution"', *Concorrenza e Mercato*, 23, 29-57.